Блейхут Р.

Теория и практика кодов, контролирующих ошибки

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Б68

Блейхут Р.
Б68 Теория и практика кодов, контролирующих ошибки / Блейхут Р. – М.: Книга по Требованию, 2013. – 566 с.

ISBN 978-5-458-30241-8

Монография известного американского специалиста, адресованная тем, кто непосредственно разрабатывает программы и аппаратуру помехоустойчивого кодирования. В ней впервые излагается разработанный автором единый подход к кодированию и декодированию, основанные на дискретном преобразовании Фурье.Дли чтения книги достаточно знать математику и объеме втузовских программ (первые главы содержат необходимые сведения по алгебре). Она может служить и основой для курсов лекций, и пособием при первоначальном ознакомлении с предметом.Для математиков-прикладников, программистов и инженеров, а также для аспирантов и студентов вузов.

ISBN 978-5-458-30241-8

ОТ РЕДАКТОРА ПЕРЕВОДА

Книга Р. Блейхута посвящена разделу науки, за которым традиционно закреплено название «теория кодов, исправляющих ошибки». В последнее время, однако, в зарубежной литературе все чаще используется более точный термин «коды, контролирующие ошибки», поскольку эта теория изучает не только исправление, но и обнаружение ошибок. В отличие от традиционных курсов теории кодирования, адресованных в первую очередь специалистам в области передачи информации, данная книга ориентирована на проектировщиков цифровых комплексов обработки данных независимо от того, для чего предназначены эти комплексы: для передачи данных, для их хранения или для других операций над ними.

Это условие наложило свой отпечаток на структуру книги. В ней почти не рассматриваются вопросы оптимальности предлагаемых методов кодирования, а вопросы их схемной реализации исследуются более подробно, чем это обычно принято. Хотя книга в первую очередь адресована читателю с инженерным образованием и формально не требует от него предварительного знакомства с высшей алгеброй, ее математический уровень достаточно высок (отметим, что в начале книги имеются специальные главы, излагающие сведения из алгебры).

Центральное место в книге занимает спектральная теория циклических кодов, в развитие которой автор внес существенный вклад. Достаточно отметить модификацию автором процедуры Берлекэмпа—Месси, позволившую сократить число операций декодирования с $O(n^2)$ до $O(n \log n)$. Эта теория излагается в гл. 8--11 и частично в гл. 13 на основе дискретного преобразования Фурье (ДПФ) в конечных полях. Хотя связь ДПФ с циклическими кодами была известна и ранее, Р. Блейхут был первым, кто заметил большие потенциальные возможности такого подхода. Этот подход не только позволяет упростить процедуру декодирования, но и способствует более глубокому пониманию теории циклических кодов.

В основном книга посвящена теории блоковых кодов, и автор излагает ее превосходно. Теория сверточных кодов излагается

несколько бегло и не всегда достаточно четко. В частности, минимальное расстояние сверточных кодов, введенное в гл. 12, мало связано с реальными характеристиками этих кодов, а их теоретическое описание неточно. Некоторые неточности содержит и гл. 15, посвященная связи модуляции и кодирования.

В списке литературы неполно отражен вклад в теорию кодирования советских ученых, так что в отдельных случаях переводчики (гл. 1, 2, 4—6 и 8—15 переведены И. И. Грушко, гл. 3 и 7 — В. М. Блиновским) сочли необходимым дать соответствующие комментарии. При переводе учтены исправления, внесенные автором в первоначальный вариант книги, и исправлены замеченные опечатки.

Переводчики и редактор выражают признательность автору книги за сотрудничество в процессе перевода книги, в частности за любезно присланное им исправленное ее издание. Соответствующие изменения внесены в перевод в корректуре.

К. Ш. Зигангиров

ПРЕДИСЛОВИЕ К РУССКОМУ ИЗДАНИЮ

Автор переведенной на иностранный язык книги чувствует себя как отец, сын которого покидает дом, чтобы начать собственную жизнь: к чувству гордости примешивается сознание, что книга начинает новую жизнь, которую ты никогда не узнаешь. Русское издание готовилось специалистами высокого класса: редактором Камилем Зигангировым и переводчиками Инной Грушко и Владимиром Блиновским. Я очень благодарен им за большую работу по переводу книги «Теория и практика кодов, контролирующих ошибки» на русский язык.

Используя возможность, предоставленную мне издательством «Мир», я обращаюсь к советскому читателю. Он несомненно заметит, что книга адресована как инженерам, так и математикам, работающим в области приложений, и что в ней декодерам и алгоритмам декодирования уделяется гораздо больше внимания, чем в других книгах. Это связано отчасти с моими научными интересами и отчасти с широким распространением декодеров, исправляющих ошибки, за последнее десятилетие. Найти хороший алгоритм декодирования сейчас так же важно, как и найти хороший код. Читатель обнаружит также, что в книге недостаточно отражен крупный вклад советских исследователей в эту область. Частично это объясняется моей неосведомленностью, частично тем, что во многих советских работах принят более высокий уровень математической строгости, чем принятый в данной книге, и, наконец, тем, что советские исследователи не столь интенсивно работают в области алгоритмов декодирования, которая интересует меня больше всего.

Я хотел бы поблагодарить переводчиков и редактора за исправление многочисленных ошибок, которые они нашли, и принимаю ответственность за оставшиеся ошибки.

Р. Э. Блейхут

ОДНИ ЛИШЬ СЛОВА — ЭТО НИЧТО
— девиз Королевского общества

ПРЕДИСЛОВИЕ

В настоящее время невозможно представить себе инженера-конструктора цифровых систем, который бы не был знаком с кодами, контролирующими ошибки. Сегодняшний интерес к этому предмету резко контрастирует с тем, что в прежние годы такие коды считались практически применимыми лишь в самых дорогих системах связи. Необходимость в контроле ошибок сейчас так велика, а возможности электроники столь развиты, что интерес к этой тематике непрерывно растет. Умение применять кодирование стало важным для любого специалиста, создающего современные системы связи или большие цифровые системы, и это умение ценится все больше. По этой теме написаны превосходные книги, но в них основное внимание уделяется математическим исследовательским аспектам. Традиционно превалируют вопросы, связанные с построением лучших кодов. Хотя эти вопросы важны для дальнейшего развития теории, конструктору в принципе интересно лишь то, что он может построить.

Эта книга написана для студентов и инженеров, которые интересуются кодами, контролирующими ошибки, и намереваются использовать их в различных приложениях. Сказав это, мы должны, однако, также сказать, что отделить практику от теории невозможно. Не располагая необходимой математической базой и опираясь лишь на поверхностное знакомство с материалом, конструктор не сможет удовлетворительно работать, хотя ему нет необходимости столь же мастерски владеть всеми аспектами теории, как исследователю.

Книга возникла из конспекта курса лекций, посвященного контролирующим ошибки кодам, который автор много раз читал как в Корнеллском университете, так и в корпорации ИБМ. От слушателей этих лекций нельзя было ожидать какой-либо подготовки по современной алгебре. Поэтому одно из требований к курсу состояло в изложении необходимых основ алгебры, которое обеспечило бы достаточную математическую строгость, и в то же время умещалось в считанное число лекционных часов. Учитывая это ограничение, я попытался включить в книгу все те основы алгебры, которые требуются для введения в теорию контролирую-

щих ошибки кодов и позволяют проводить доказательства или убедительную аргументацию. Это тот минимум, без которого инженер не может быть уверен в своих построениях.

На протяжении тех лет, что читался курс, аудитория изменилась: сначала это были аспиранты и студенты старших курсов, а затем появились и студенты младших курсов; это заставило заботиться о более простых объяснениях, излагавшихся, по возможности, на языке, понятном инженерам. Математические рассуждения проводились на возможно более низком уровне, хотя в некоторых вопросах уровень оставался достаточно высоким.

Материал излагается в форме «теорема—доказательство», хотя в инженерной литературе чаще используется описательная форма. Принятая нами форма позволяет читателю при желании пропускать доказательства и выделять необходимые главные факты. Кроме того, те, кто заботится о строгости, могут разбить теорию на легче усваиваемые части.

Я пытался выдвинуть на первый план преобразование Фурье в конечных полях, так как оно интуитивно понятнее инженерам и быстро усваивается людьми с техническим образованием. Применение преобразования Фурье проясняет также тот факт, что теория контролирующих ошибки кодов является одной из ветвей теории дискретной обработки сигналов. Хотя для студентов инженерных специальностей предпочтительнее другой способ изложения того же круга идей, который основан на использовании многочленов Мэттсона—Соломона, такое изложение вызвало бы необходимость изучать новый для них язык в то время, как они уже владеют одним, столь же употребительным.

По возможности подчеркивалась тесная связь теории кодов, контролирующих ошибки, и теории обработки дискретных сигналов. Во многих работах эта связь оставалась невыявленной; объяснение заключается в том, что данные дисциплины развивались совершенно различными путями: одна разрабатывалась в основном алгебраистами, а другая — в основном инженерами. Однако, если не считать различия в числовых системах — поле Галуа в одном случае и поле комплексных чисел в другом — используемые методы аналогичны. Обе дисциплины основаны на преобразовании Фурье, фильтрах с конечным импульсным откликом, циклических свертках и соотношениях между свойствами последовательностей во временной и частотной областях.

В книге на первый план выдвигается реализация кодеров и декодеров с помощью цепей, содержащих регистры сдвигов, причем по возможности используется техническая терминология, принятая в теории фильтров. Для максимально возможной ясности изложения описывается построение регистров сдвига и часто выявляются модификации, позволяющие уменьшить число элементов устройства. Даже в тех случаях, когда описывается про-

граммная реализация кодеров и декодеров, приводятся некоторые соображения о том, как использование регистров сдвига может упростить программу. Моя точка зрения состоит в том, что окончательным критерием качества кода или алгоритма является стоимость кодера и декодера. Инженер не будет интересоваться кодами с наибольшим минимальным расстоянием, если неизвестны хорошие алгоритмы их декодирования. Хорошие коды нуждаются в хорошем декодере, а хорошие алгоритмы декодирования найти трудно. По-видимому, поиск теоретиками новых кодов, допускающих использование известных алгоритмов декодирования, может оказаться более плодотворным, нежели поиск новых алгоритмов декодирования для известных кодов.

При выборе обозначений и терминологии всегда возникает вопрос, использовать ли традиционные или ввести новые, более удобные. В выборе обозначений предпочтение отдается традиционным, хотя в некоторых случаях я считал, что важнее добиться методологической ясности и согласованности. Например, при обсуждении сверточных кодов я выбрал обозначения, подчеркивающие их аналогию с блоковыми кодами, хотя иногда они отличаются от обозначений, принятых в литературе по сверточным кодам.

Благодарности. Было бы очень трудно перечислить все беседы и источники, оказавшие существенное влияние на эту книгу: любой список оказался бы неполным, и поэтому я упомяну лишь главные.

Профессор Тоби Бергер был моим другом и консультантом на протяжении всех лет работы над книгой: его советы всегда были очень полезны. Профессор Д. Л. Сервейт внимательно прочитал большую часть рукописи и спас меня от многих ошибок и неточностей. Полезные советы и критические замечания сделали также К. Л. Чинь, А. ЭльГамаль, М. Р. Бест, Н. М. Блечман, Т. Хасимото, К. Кобаяси, М. Симада, Г. Унгербёк, В. Вандеркулк, С. Виноград и С. К. Вест. Книги и статьи, прямо или косвенно оказавшие существенное влияние на нашу книгу, перечислены в списке литературы; список статей, оказавших меньшее влияние, был бы необъятным.

Я должен выразить признательность корпорации ИБМ за поддержку при подготовке этой книги и Корнеллскому университету за предоставление лекционных помещений, в которых ее текст прошел апробацию. Текст книги шлифовался также в процессе лекций, прочитанных в Технологическом институте Южного Китая.

Наиболее важное участие в подготовке книги приняла моя жена Барбара. Она помогала и морально поддерживала меня, разделяя все трудности и удачи. Наконец, эта книга посвящается Эдварду Дж. Блейхуту, Эндрю С. Чамеру и Карлу А. Крачепфелсу; частицы их душ живут в ней.

ГЛАВА 1
ВВЕДЕНИЕ

Обработка дискретных сигналов является инженерной дисциплиной со многими разветвлениями. Сюда относится и теория кодов, контролирующих ошибки, — отдельный предмет со своими собственными задачами и собственными арифметическими системами. Однако наиболее эффективными из этих арифметических систем являются известные операции обработки сигналов, в том числе свертки, преобразования Фурье, фильтры и регистры сдвигов. Теория кодов, контролирующих ошибки, - - предмет со своей собственной историей и своими прелестями; его различные грани смыкаются со многими другими дисциплинами.

Рассматриваемая в теории кодов, контролирующих ошибки, техническая задача состоит в защите цифровых данных от появляющихся в процессе передачи по каналам связи ошибок. Многие хитроумные способы защиты от ошибок, развитые на основе богатой математической теории, превратились в зрелые важные инженерные методы с многочисленными приложениями.

Большие объемы данных в современных системах связи и хранения данных, большинство из которых очень чувствительно к ошибкам, приводят к необходимости контроля ошибок. Зрелая теория хороших кодов и хороших кодовых алгоритмов способна удовлетворить эту потребность. Кроме того, быстрые успехи в создании интегральных цифровых схем открывают возможность реализации этих алгоритмов.

1.1. ДИСКРЕТНЫЙ КАНАЛ СВЯЗИ

Система связи соединяет источник данных с получателем данных посредством канала; примерами каналов являются микроволновые линии, коаксиальные кабели, телефонные сети и даже магнитные ленты. При проектировании системы связи разрабатываются устройства, подготавливающие вход и обрабатывающие выход каналов. Уже стало традицией подразделять основные функции

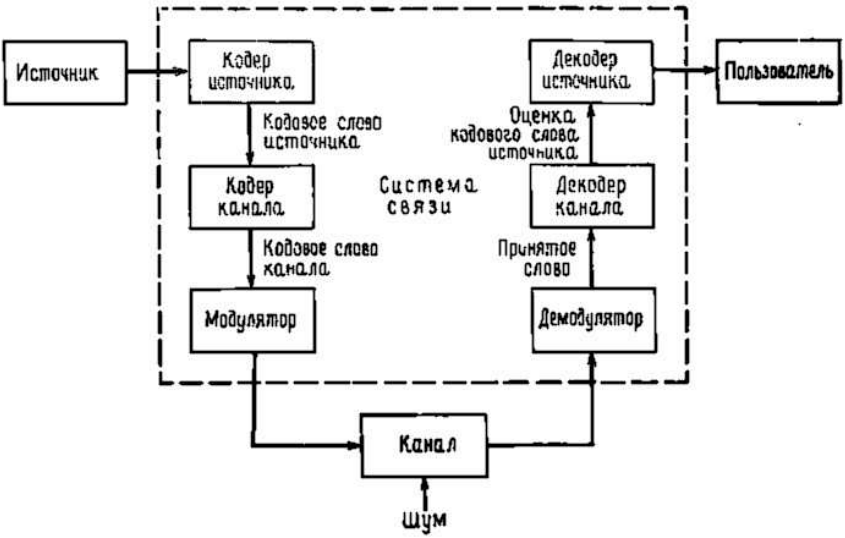

Рис. 1.1. Блок-схема цифровой системы связи.

цифровой системы связи так, как показано на блок-схеме на рис. 1.1.

Данные, поступающие в систему связи от источника данных, прежде всего обрабатываются кодером источника, предназначенным для более компактного представления данных источника. Это промежуточное представление является последовательностью символов, которая называется *кодовым словом источника*. Затем данные обрабатываются кодером канала, преобразующим последовательность символов кодового слова источника в другую последовательность символов, называемую *кодовым словом канала*. Кодовое слово канала представляет собой новую, более длинную последовательность с большей, чем у кодового источника, избыточностью. Каждый символ кодового слова канала может быть представлен битом или, возможно, группой битов.

Далее модулятор преобразует каждый символ кодового слова канала в соответствующий аналоговый символ из конечного множества допустимых аналоговых символов. Последовательность аналоговых символов передается по каналу. Так как в канале возникают различного типа шумы, искажения и интерференция, то выход канала отличается от его входа. Демодулятор преобразует каждый полученный на выходе канала сигнал в последовательность символов одного из кодовых слов канала. Каждый принятый символ является лучшей оценкой переданного символа, но из-за шума в канале демодулятор делает ошибки. Демодулиро-

ванная последовательность символов называется *принятым словом*. Из-за ошибок символы принятого слова не всегда соответствуют символам кодового слова канала.

Декодер канала использует избыточность кодового слова канала для того, чтобы исправить ошибки в принятом слове, и затем выдает оценку кодового слова источника. Если все ошибки исправлены, то оценка кодового слова источника совпадает с исходным кодовым словом источника. Декодер источника выполняет операцию, обратную операции кодера источника, результат которой поступает к получателю.

В данной книге рассматривается только конструкция кодера и декодера канала — дисциплина, известная как *кодирование, контролирующее ошибки*. Сжатие данных или функции более компактной записи данных, выполняемые кодером и декодером источника, а также устройства модулятора и демодулятора в ней не рассматриваются. Кодер и декодер канала будут в дальнейшем называться просто кодером и декодером соответственно.

1.2. ИСТОРИЯ КОДИРОВАНИЯ, КОНТРОЛИРУЮЩЕГО ОШИБКИ

История кодирования, контролирующего ошибки, началась в 1948 г. публикацией знаменитой статьи Клода Шеннона. Шеннон показал, что с каждым каналом связано измеряемое в битах в секунду и называемое *пропускной способностью* канала число C, имеющее следующее значение. Если требуемая от системы связи скорость передачи информации R (измеряемая в битах в секунду) меньше C, то, используя коды, контролирующие ошибки, для данного канала можно построить такую систему связи, что вероятность ошибки на выходе будет сколь угодно мала. В самом деле, из шенноновской теории информации следует тот важный вывод, что построение слишком хороших каналов является расточительством; экономически выгоднее использовать кодирование. Шеннон, однако, не указал, как найти подходящие коды, а лишь доказал их существование. В пятидесятые годы много усилий было потрачено на попытки построения в явном виде классов кодов, позволяющих получить обещанную сколь угодно малую вероятность ошибки, но результаты были скудными. В следующем десятилетии решению этой увлекательной задачи уделялось меньше внимания; вместо этого исследователи кодов предприняли длительную атаку по двум основным направлениям.

Первое направление носило чисто алгебраический характер и преимущественно рассматривало *блоковые коды*. Первые блоковые коды были введены в 1950 г., когда Хэмминг описал класс блоковых кодов, исправляющих одиночные ошибки. Коды Хэмминга были разочаровывающе слабы по сравнению с обещанными

Шенноном гораздо более сильными кодами. Несмотря на усиленные исследования, до конца пятидесятых годов не было построено лучшего класса кодов. В течение этого периода без какой-либо общей теории были найдены многие коды с малой длиной блока. Основной сдвиг произошел, когда Боуз и Рой-Чоудхури [1960] и Хоквингем [1959] нашли большой класс кодов, исправляющих кратные ошибки (коды БЧХ), а Рид и Соломон [1960] нашли связанный с кодами БЧХ класс кодов для недвоичных каналов. Хотя эти коды остаются среди наиболее важных классов кодов, общая теория блоковых кодов, контролирующих ошибки, с тех пор успешно развивалась, и время от времени удавалось открывать новые коды.

Открытие кодов БЧХ привело к поиску практических методов построения жестких или мягких реализаций кодеров и декодеров. Первый хороший алгоритм был предложен Питерсоном. Впоследствии мощный алгоритм выполнения описанных Питерсоном вычислений был предложен Берлекэмпом и Месси, и их реализация вошла в практику как только стала доступной новая цифровая техника.

Второе направление исследований по кодированию носило скорее вероятностный характер. Ранние исследования были связаны с оценками вероятностей ошибки для лучших семейств блоковых кодов, несмотря на то что эти лучшие коды не были известны. С этими исследованиями были связаны попытки понять кодирование и декодирование с вероятностной точки зрения, и эти попытки привели к появлению последовательного декодирования. В последовательном декодировании вводится класс неблоковых кодов бесконечной длины, которые можно описать деревом и декодировать с помощью алгоритмов поиска по дереву. Наиболее полезными древовидными кодами являются коды с тонкой структурой, известные под названием *сверточных кодов*. Эти коды можно генерировать с помощью цепей линейных регистров сдвига, выполняющих операцию свертки информационной последовательности. В конце 50-х годов для сверточных кодов были успешно разработаны алгоритмы последовательного декодирования. Интересно, что наиболее простой алгоритм декодирования — алгоритм Витерби — не был разработан для этих кодов до 1967 г. Применительно к сверточным кодам умеренной сложности алгоритм Витерби пользуется широкой популярностью, но для более мощных сверточных кодов он не практичен.

В 70-х годах эти два направления исследований опять стали переплетаться. Теорией сверточных кодов занялись алгебраисты, представившие ее в новом свете. В теории блоковых кодов за это время удалось приблизиться к кодам, обещанным Шенноном: были предложены две различные схемы кодирования (одна Юстесеном, а другая Гоппой), позволяющие строить семейства кодов,